保安資訊--本周(台灣時間2022/02/25)賽門鐵克原廠防護公告重點說明

前言

賽門鐵克原廠首要任務就是保護我們的顧客，被譽為賽門鐵克解決方案專家的保安資訊更能發揮我們被高度認可的專業知識與技能、豐富經驗以及專為幫助客戶成功的服務熱忱，與顧客共同創造賽門鐵克解決方案的最大效益，並落實最佳實務的安全防護。攻擊者從不休息，我們更不會。一支技術精湛且敬業的團隊不斷創造新的防護措施，以應對每天發布成千上萬的新威脅。儘管不可能詳述我們已經可以防禦的每種新威脅，但該站點至少反映了我們的努力。這些公告分享針對當前熱門新聞話題有關威脅的保護更新，確保您已知道自己受到最佳的保護。點擊此處獲取賽門鐵克原廠防護公告(Protection Bulletins)。

關於 保安資訊有限公司 | 從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

在端點啟用賽門鐵克入侵預防系統(IPS) 的好處(以下皆為美國時間)

賽門鐵克的入侵預防系統(IPS)是業界一流的深層封包檢測技術引擎，可保護包括財富 500 強企業和消費者在內的數億個端點(桌機／筆電／伺服主機)。

過去的 7 天內，SEP 的網路層保護引擎 (IPS) 在 130 萬個受保護端點上總共阻止了 2.0463 億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/02/22)**

- 在**23萬6,300**台端點上，阻止了**1.031**億次嘗試掃描**Web**服務器的漏洞。
- 在**50萬9,200**台端點上，阻止了**4,430**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**8萬8,500**台**Windows**伺服主機上，阻止了**2,590**萬次攻擊。
- 在**18萬7,100**端點上，阻止了**1,010**萬次嘗試掃描伺服器漏洞。
- 在**10萬3,300**台端點上，阻止了**490**萬次嘗試掃描在**CMS**漏洞。
- 在**15萬1,400**台端點上，阻止了**400**萬次嘗試利用的應用程式漏洞。
- 在**47萬7,400**台端點上，阻止了**1,300**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**4,700**台端點上，阻止了**450**萬次加密貨幣挖礦攻擊。
- 在**13萬2,700**台端點上，阻止了**540**萬次向惡意軟體**C&C**連線的嘗試。
- 在**7,600**台端點上，阻止了**27萬400**次加密勒索嘗試。

強烈建議用戶在桌機／筆電／伺服主機上啟用 IPS (不要只把SEP/SES當一般的掃毒工具用，它有多個超強的主被動安全引擎，在安全配置正確下，駭客會知難而退)，以獲得最佳保護。點擊此處獲取有關啟用 IPS 的說明，或與保安資訊聯繫可獲得最快最有效的協助。

2022/02/24

困擾MacOS用戶--惡意廣告軟體載入程式：AdLoad

多年來，眾所周知，在 MacOS 威脅環境中觀察到的廣告軟體變得不僅更先進，還更有耐心。一個惡名昭彰的廣告軟體載入程式--AdLoad，隨著其流行程度的增加，繼續在新聞和社交媒體中看到。賽門鐵克每天跟蹤 Adload（及其變種）活動，繼續透過偷渡下載散播，同時偽裝成假冒的熱門應用程式 Apps。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- OSX.AdLoad
- OSX.AdLoad!g1

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- System Infected: OSX Hydromac Activity
- System Infected: OSX.Trojan.Gen Activity 1

2022/02/24

古巴勒索軟體幕後的威脅者，利用各種漏洞作為其攻擊的手段

據報導，古巴勒索軟體幕後的威脅者--UNC2596 越來越常利用各種漏洞作為其攻擊的初始感染媒介。在去年一些與古巴勒索軟體有關行動中，UNC2596 一直在利用 MS Exchange ProxyLogon 漏洞。據瞭解，該威脅集團還使用各種偵察工具和不同的惡意軟體變種，其中包括：Cobalt Strike、Wedgecut 偵查工具、Bughatch下載程式或 Termite 植入程式。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt
- Backdoor.Cobalt!gen11
- Backdoor.Cobalt!gen12
- CL.Downloader!gen12
- Downloader
- ISB.Downloader!gen80
- Ransom.Cuba
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Web Attack: Webpulse Bad Reputation Domain Request

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2022/02/24

Lucifer (*路西法／*晨星)--簡單的竊密程式和爬蟲程式

威脅領域不乏竊密程式和爬蟲程式，最容易出現在一些團體和個人花錢利用此類惡意軟體。這個自由市場幾乎每天都在不斷成長，讓各種技能水平的網路犯罪分子百家爭鳴，也會把一些好奇的靈魂轉向黑暗面。最近一個名為 Lucifer 的竊密程式被破解並被散發。它是一個基本的竊密程式，又有機器人功能，能夠竊取儲存在主流網頁瀏覽器中的密碼並獲取 FTP 密碼。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspBeh!gen616
- SONAR.SuspTempRun
- SONAR.SuspTempRun2

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/02/23

網路也是戰場--針對烏克蘭的新型磁碟清除程式

我們知道有報導一個關於針對烏克蘭的新型磁碟清除程式。該磁碟清除程式的數位簽章是由 Hermetica Digital Ltd 簽發，以確立其合法性。該磁碟清除程式置入一個由帶有 EaseUp Partition Master 數位簽章的合法磁碟清除驅動程式，以執行磁碟清除功能。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.2
- Trojan Horse
- Trojan.Killdisk
- WS.Malware.2

基於安全強化政策(適用於使用DCS)：

DCS 內建的強化安全政策早已能預防安裝被安裝 Trojan.KillDisk 及其惡意行為並提供零時差攻擊提供保護。

2022/02/23

不斷翻新的 SugarLocker 勒索軟體，不容小覷

SugarLocker 勒索軟體營運商已經被觀察到，在暗網上以“gustavedore”用戶名稱為新的合作夥伴投放廣告。SugarLocker 使用可高度客製化的勒索軟體即服務 (RaaS) 營運模式。該模式正在不斷翻新，因此一旦找到更多合作夥伴，我們可能會觀察到更多活動。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(Snoar)的防護：

- Ransom.Encoded!gm1

郵件安全防護機制：

不管是地端自建(SMG／SMSEX)的郵件過濾／安全閘道及主機防護、雲端郵件安全服務(E-mail Security.Cloud)以及郵件威脅隔離(ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護(威脅不落地)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Trojan.Backdoor Activity 634

2022/02/23

Mars (*火星) 竊密程式，在網路威脅版圖仍然活躍

Mars (*火星) 竊密程式早在 2021 年就被首次發現，它是基於一個被稱為 Oski 的舊版竊密程式。Mars (*火星) 正在幾個地下論壇上出售，據說還在不斷開發中。該惡意軟體目標是儲存在各種瀏覽器中的用戶帳密，以及大量不同的加密貨幣錢包。Mars (*火星) 竊密程式正在透過各種手段進行傳播，包括：社交工程技術、惡意廣告行動、惡意破解軟體和序號產生器。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- MSIL.Downloader!gen7
- Trojan Horse
- Trojan.Gen.2
- W97M.Downloader

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Web Attack: Webpulse Bad Reputation Domain Request

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2022/02/22

新版 CryptBot 竊密程式，具有從 Chrome 瀏覽器中竊取瀏覽器資訊等能力

根據最近發佈的一份報告，CryptBot 惡意軟體一個新的修改版本已經在真實網路世界出現。CryptBot 是一支竊密程式，具有獨特的反沙箱和反虛擬機器技術。最新的變種包括一些功能升級，如從 Chrome 瀏覽器中竊取瀏覽器資訊，包括最新的版本。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.2
- Trojan.Gen.MBT

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Web Attack: Webpulse Bad Reputation Domain Request

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2022/02/22

MacOS 加密貨幣挖礦惡意程式，利用I2P網路隱藏其通信內容

一個針對 MacOS 平臺新的加密貨幣挖礦惡意程式變種已經被發現。該惡意軟體被懷疑是透過偽裝成 Adobe Photoshop 安裝程式的 .DMG 蘋果磁碟映像檔傳遞。該挖礦惡意程式使用幾個修改過的開放原始碼元件進行惡意攻擊，並使用 i2pd (又名 I2P Daemon)，以允許匿名的點對點加密通信，來隱藏其網路流量而聞名。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- OSX.Trojan.Gen
- OSX.Trojan.Gen.2

2022/02/21

針對 MS-SQL 伺服器的 Cobalt Strike 散播行動

根據最近報導，一個新的攻擊行動正在散播 Cobalt Strike beacons (信標)，該行動的目的在針對有漏洞的 MS-SQL 伺服器。這些變種是透過 MS-SQL 程序的 cmd.exe 和 powerhell.exe 命令下載。一旦下載，該惡意軟體就能夠注入合法的應用程式，以逃避安全軟體的檢測。Cobalt Strike 是一個商業滲透測試工具，被用作散播早期的初始攻擊的媒介，進一步傳播惡意的有效籌載，例如：遠端存取木馬 (RATs)、挖礦軟體和勒索軟體。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt
- MSIL.Packed.25
- Scr.Malcode!gdn30
- Trojan.Gen.MBT

基於行為偵測技術(Snoar)的防護：

- Backdoor.Cobalt!gm
- Backdoor.Cobalt!gm1

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Web Attack: Webpulse Bad Reputation Domain Request

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2022/02/21

SharkBot V1.63--行動惡意軟體推出新變種，重出江湖

一個名為 SharkBot v1.63 安卓 (Android) 惡意軟體的新版本已在真實世界被發現。Sharkbot 在 2021 年 10 月前後首次出現，是一個銀行木馬的變種，能夠進行金融欺詐和竊取客戶的敏感資訊。該惡意軟體利用自動轉帳系統 (ATS) 的功能，在各種銀行應用程式中自動填寫表格，並繞過多因素認證，從被入侵的裝置中進行欺詐性的金融轉帳。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

賽門鐵克的端點防護行動裝置版本(IOS/Android)已將其歸類為以下威脅並提供最完善的保護能力：

賽門鐵克的端點防護行動裝置版本 (IOS/Android) 還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 重要來源之一 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊 (SMS) 網路釣魚攻擊。

- Android.Reputation.2
- AppRisk:Generisk

2022/02/20

Teardroid (*淚滴)--具有遠端存取和盜竊功能的 Android(*安卓) 機器人

Teardroid (*淚滴) 是一個具有遠端存取和盜竊功能的 Android (安卓) 機器人，已經存在好幾年了，最近發佈第四版。然而，從行動威脅的角度來看，這個機器人並不像 Flubot、Medusa、Joker、Anubis 等惡名昭彰的威脅那樣流行。透過受歡迎的網際網路託管平臺上進行軟體發展和版本控制，有一些團體和個人繼續利用它。它也被「鏡像 (Mirror Site)」到駭客論壇和網站上。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

賽門鐵克的端點防護行動裝置版本(IOS/Android)已將其歸類為以下威脅並提供最完善的保護能力：

賽門鐵克的端點防護行動裝置版本 (IOS/Android) 還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 重要來源之一 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊 (SMS) 網路釣魚攻擊。

- AppRisk:Generisk